UNITED STATES DISTRICT COURT

for the

Eastern District of Wisconsin

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)
Items 1-12 as described in ATTACHMENT A

Case No. 21M649

APPLICATION FOR A WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location):*

Items 1-12 as described in ATTACHMENT A

located in the Eastern District of Wisconsin, there is now concealed *(identify the person or describe the property to be seized):*

Please see attached affidavit and ATTACHMENT B.

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☑ contraband, fruits of crime, or other items illegally possessed;
- ☑ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
Title 18, United States Code, Sections 1708, 514(a), 1028A, 1029, and 371.	Mail Theft (18 USC 1708), Fictitious Obligations (18 USC 514(a)), Aggravated Identity Theft (18 USC 1028A), Access Device Fraud (18 USC 1029), and Conspiracy (18 USC 371)

The application is based on these facts:

See attached affidavit and ATTACHMENTS A and B.

- ☑ Continued on the attached sheet.
- ☐ Delayed notice of _____ days *(give exact ending date if more than 30 days:* _____ *)* is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

1:19PM

Applicant's signature

MATT SCHMITZ, U.S. POSTAL INSPECTOR

Printed name and title

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by _____ *(specify reliable electronic means).*

Date: 4-5-2021

Judge's signature

City and state: Green Bay, WI

U.S. Magistrate Judge, Hon. James R. Sickel

Printed name and title

AFFIDAVIT

I, Matthew Schmitz, United States Postal Inspector, being duly sworn, state the following information was developed from the Affiant's personal knowledge and from information furnished to the Affiant by other law enforcement agents and business contacts:

I. INTRODUCTION

1. I have been a Postal Inspector with the United States Postal Inspection Service for approximately 17 years and am currently assigned to the Green Bay (WI) Domicile in the Eastern District of Wisconsin. Before becoming a Postal Inspector I served as a police officer with the Janesville Police Department in Janesville, Wisconsin for one year and as a police officer and detective with the Middleton Police Department in Middleton, Wisconsin for approximately five years. As a Postal Inspector I am responsible for investigating criminal violations that involve the United States Mail and United States Postal Service. These investigations include, but are not limited to, mail fraud, mail theft, credit card fraud, identity theft, personal and business check forgeries, controlled substance distribution, burglaries and robberies of United States Postal Service facilities and its employees, and conspiracies regarding those offenses. I have conducted mail theft investigations that have also involved the theft of gift cards, credit cards, personal and business checks, debit cards, and personal identifying information (PII) contained within those stolen mailings.

PURPOSE

2. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a search warrant authorizing the examination of property—described in Attachment A—which is currently in law enforcement possession, and the extraction from that property of electronically stored information described in Attachment B. This affidavit is intended to show only that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

3. The property to be searched as identified in ATTACHMENT A is currently in the possession of the Grand Chute Police Department in Grand Chute, WI. Therefore, all property to be searched as listed in ATTACHMENT A is

currently located in the Eastern District of Wisconsin. This warrant would authorize the forensic examination of the property listed in ATTACHMENT A for the purpose of identifying electronically stored data particularly described in ATTACHMENT B.

DEFINITIONS

4. Based on my training and experience, I use the following technical terms to convey the following meanings:

   a. Cellular Telephone or Cellular Devices: A cellular telephone (or mobile telephone, or wireless telephone) is a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional "land line" telephones. A wireless telephone usually contains a "call log," which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic "address books;" sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Wireless telephones may also include global positioning system ("GPS") technology for determining the location of the device.

   b. Internet: The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

   c. Tablet: A tablet is a mobile computer, typically larger than a phone yet smaller than a notebook, that is primarily operated by touching the screen. Tablets function as wireless communication devices and can be used to access the Internet through cellular networks, 802.11 "wi-fi" networks, or otherwise. Tablets typically contain programs called apps, which, like programs on a personal computer, perform different

functions and save data associated with those functions. Apps can, for example, permit accessing the Web, sending and receiving e-mail, and participating in Internet social networks.

d. IP Address: An Internet Protocol address (or simply "IP address") is a unique numeric address used by computers on the Internet. An IP address is a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer attached to the Internet computer must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static—that is, long-term—IP addresses, while other computers have dynamic—that is, frequently changed—IP addresses.

COMPUTERS AND ELECTRONIC STORAGE

5. This warrant seeks the Court's permission to search and seize records as identified in ATTACHMENT B that might be found on the property identified in ATTACHMENT A, in whatever form it is found. I submit that there is probable cause to believe the evidence described in ATTACHMENT B will be stored on the property identified in ATTACHMENT B based upon the facts provided in this affidavit and for the following reasons:

a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a hard drive, deleted or viewed via the Internet. Electronic files downloaded to a hard drive can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using readily available forensics tools. This is so because when a person "deletes" a file on a home computer, the data contained in the file does not actually disappear; rather, that data remains on the hard drive until it is overwritten by new data.

b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the hard drive that is not currently being used by an active file—for long periods of time before they are

overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

c. Similarly, files that have been viewed via the Internet are typically automatically downloaded into a temporary Internet directory or "cache." The browser often maintains a fixed amount of hard drive space devoted to these files, and the files are only overwritten as they are replaced with more recently viewed Internet pages or if a user takes steps to delete them.

6. I know from my training and investigative experience that when an individual uses a computer to produce counterfeit documents, checks, identification cards, and other instrumentalities in furtherance of the scheme, that computer will generally serve both as an instrumentality for committing the crime, and also as a storage device for evidence of the crime. The computer is an instrumentality of the crime because it is used as a means of committing the criminal offense. The computer is also likely to be a storage device for evidence of crime. From my training and experience, I believe that a computer used to commit a crime of this type may contain: data that is evidence of how the computer was used; data that was sent or received; notes as to how the criminal conduct was achieved; records of Internet discussions about the crime; and other records that indicate the nature of the offense.

FACTS

7. Since approximately November, 2020, I have worked an investigation involving mail theft, check fraud, identity theft, and bank fraud. During the course of this investigation I received information from numerous law enforcement agencies in northeast and central Wisconsin about individuals who they were investigating for incidents of mail theft, check fraud, and identity theft. I also gathered information through my own investigation of these incidents and from interviews with individuals suspected of being involved in this scheme that several individuals were suspected of being involved in a large scheme centered on the theft of US Mail for the purpose of obtaining checks, personal identifying information, and credit/debit card

information. One of the individuals identified through interviews and bank surveillance video as being involved in stealing mail and cashing counterfeit checks is Pao Yang.

8. During the course of this investigation I had contact with Outagamie County Sheriff's Sgt. John Schuette regarding his investigation of Taylor Cooley. In January, 2021, the Whistle Inn bar in Nichols, WI reported several checks drawn on their Fox Communities Credit Union (FCCU) account had been fraudulently cashed at FCCU locations in the Appleton, WI area. Sgt. Schuette and I determined through contact with the owners of the Whistle Inn bar that a check drawn on their FCCU account had been stolen from their residential mailbox in rural Black Creek, WI, on or about January 11, 2021. This check, check number 3437 payable for $100, was being mailed to pay dues to a local motorcycle club.

9. FCCU staff provided records to law enforcement showing an individual identifying himself by his Wisconsin driver's license as Taylor D Cooley of Appleton, WI had presented for payment (cash) Whistle Inn check numbers 3471 and 3472 payable for $1,150 and $800, respectively. Cooley also attempted to cash a third check, check number 3411 for $800, but drove away and left his driver's license and check with the teller. Sgt. Schuette made contact with Cooley regarding the checks and arrested him on warrants he had through Brown County.

10. On January 28, 2021, Sgt. Schuette and I made contact with Cooley at the Outagamie County Jail in Appleton, WI and conducted a post-Miranda interview. Cooley said in December, 2020, he met two male Asians he knew as Pao "Trick" Yang and Kao "Loki" Thor through his friend, Brittany Webie. One evening in or around the end of December, 2020, after the group (Pao, Kao, Brittany, and Taylor) visited the Oneida Casino at 2100 Airport Dr in Green Bay, WI, Taylor said Pao drove in a rural area west of the casino (Oneida/Hobart communities) while he and Brittany were in the back seat. Pao drove up to mailboxes that had the "flag" up and Kao removed the mail from the boxes. Initially, Cooley thought they were gathering

items from the mailboxes on behalf of friends, but soon realized they were likely stealing US Mail. Cooley said on several occasions Pao and Kao provided him with methamphetamine to smoke.

11. In January, 2021, Cooley met with Kao Thor (Loki) at a residence in Neenah, WI. Kao told him if he wanted to smoke more methamphetamine he needed to help him (Kao) cash checks. Kao produced several checks payable to Cooley and directed him to go to the Fox Communities Credit Union to cash them. Cooley went alone and drove his own car. He cashed two of the checks but became nervous while trying to cash the third and abruptly left the drive-thru lane. He returned to the Neenah residence and gave Kao all of the cash he received from cashing the checks.

12. On March 21, 2021, at approximately 2:30 AM, Grand Chute Police arrested Ger Vang outside the Country Inn & Suites hotel for an outstanding warrant through Outagamie County for a methamphetamine offense and bail jumping. Pursuant to Ger's arrest, Grand Chute Police searched a vehicle Ger had operated and seized the following items:

a. Numerous checks folded in between identification documents in the names of various individuals.
b. Personal checks in the names of various individuals.
c. VersaCheck receipt in the name of Pao Yang.
d. A document scanning device.
e. A black MSI laptop computer.
f. A white Hp printer with serial number CN06A6P2X0.
g. A gray Motorolla Tracfone.
h. An LG Tracfone.
i. A black Diamondback 9mm handgun containing a magazine that held five round of ammunition.
j. A suspected methamphetamine smoking pipe.

13. Grand Chute Police determined the vehicle Ger had been operating was rented by Pao Yang. They also determined from information provided by the Country Inn & Suites that Pao Yang had rented room 204 at the hotel. Grand Chute Police Detective Katie Keuler told me as officers were making contact with Ger Vang they saw an Asian male near the entrance to the hotel that wore a flat brimmed baseball style hat. This male walked into the hotel once officers made eye contact with him. Grand Chute Police believed that based upon this male's reaction to police presence that he had been with Ger shortly before police arrived. During the course of this investigation I have learned that the subject identified by Taylor Cooley as "Trick", aka Pao Yang, is an Asian male who commonly wears baseball hats with a flat brim.

14. On March 21, 2021, immediately following Ger Vang's arrest, Grand Chute Police established surveillance at the Country Inn & Suites in an attempt to identify Pao Yang leaving the hotel. Pao was known to have an active arrest warrant through the Wisconsin Department of Corrections/Probation and Parole. At approximately 10:30 AM, Grand Chute Police saw a Honda CR-V with South Carolina license plates drive up next to the Toyota that Ger had been operating when he was arrested earlier that morning. A male, later identified as Chou Vang, exited the Honda and appeared to be using a tool to attempt to gain entry into the Toyota. When this male saw marked Grand Chute Police patrol cars approaching he got back into the Honda CR-V. Grand Chute Police made contact with the CR-V before it left the parking lot and identified the driver as Valentine Thor and passenger as Chou Vang. Chou told Grand Chute Police his "cousin", Pao, had called him to ask for assistance in gaining access to his car that was in the hotel parking lot. Valentine Thor was identified as a resident of South Carolina and said she was dating Chou.

15. When Grand Chute Police contacted Valenine and Chou in their vehicle they reported detecting an odor of marijuana. A Kaukauna Police Department certified drug detection K-9 was deployed on the exterior of the Honda CR-V and the K-9 officer, Officer Meyer, reported his K-9 alerted to the odor of controlled

substances in the vehicle. Grand Chute Police searched the vehicle pursuant to the K-9 alert and seized the following items:

a. Approximately 2 pounds of a white crystalline substance suspected of being methamphetamine.

b. Suspected controlled substance paraphernalia.

c. Various Walmart store receipts.

d. Various identification documents and checks in the names of other individuals.

e. A black 9mm handgun containing a magazine that held 14 9mm rounds.

f. A T-Mobile Revvl cell phone.

g. A blue cell phone with a pop socket (a pop socket is essentially a knob on the back of the cell phone).

h. A black Apple iPhone.

i. A Samsung cell phone with IMEI 355181113973829.

j. A Cricut Explore Air 2 label making machine.

k. A Samsung Tab S6 Lite computer tablet.

l. A Samsung Tab S7 computer tablet.

m. An Hp laptop with model number 15-dy207lwm.

n. A Notebook PC model GA5021.

o. A 12" moto bike, hoverboard, security cameras, electronic tissue massager, portable heater, five boxes containing a handheld auto vacuum, Bose headphones, and two packages of Samsung earbuds.

16. Grand Chute Police reported Chou later reported in a post-Miranda interview that he had received some of the property police had located on his person and in the vehicle from "Pao Vang, his sister's husband's brother who lived in Appleton." Specifically, Chou reported two identification documents found on his person were given to him by Pao to "hold on to." Chou also said he had let Pao borrow the vehicle the previous evening (March 20, 2021) and, upon Pao returning it, Chou noticed he (Pao) had left some of his

items in the car including a backpack, safe, checkbooks, identification documents, and a handgun. Grand Chute Police reported the two pounds of suspected methamphetamine was located within the backpack that Chou identified.

17. During the course of this investigation I had contact with Walmart Global Investigator Edward Henkel and Fiserv Senior Technical Fraud Investigator Eric Scherdel regarding a group they had identified that was making purchases of high dollar merchandise from Walmart stores and later returning the merchandise at other Walmart stores, including stores in South Carolina. Specifically, Investigator Henkel and Scherdel said several individuals were purchasing the merchandise using counterfeit checks.

18. During the course of this investigation I have reviewed investigative reports and photographs of evidence related to the investigations concerning Pao Yang and others and their suspected involvement in a large mail theft, identity theft, and check fraud scheme. I determined from those reports and the evidence seized that the individuals involved in this scheme appear to be stealing and opening U.S. Mail to obtain checks, credit cards, debit cards, and PII. In particular, checks that are stolen from the mail are later reproduced or "washed" so that new information (payee, dollar amount, check date) can be written or printed on the check and later cashed at bank or used at retail locations. I am aware from my training and investigative experience that mail theft schemes targeting mailings that likely contain personal or business checks commonly use the stolen check/s to reproduce counterfeit checks or to remove the existing payment information through "washing," a process in which household chemicals are used to lift or erase the ink on a check and then, once dried, write new information on the check. Further, based upon my training, investigative experience, and the facts presented in this affidavit, I believe Pao Yang, Ger Vang, Chou Vang, Valentine Thor, and others are using proceeds they obtain from stealing mail and forging and counterfeiting checks and credit contained within that stolen mail to purchase methamphetamine. I believe this is true considering (1) suspected methamphetamine and/or associated paraphernalia was found during the arrests of

Ger Vang, Chou Vang, and Valentine Thor on March 21, 2021, and (2) I have learned through my training and investigative experience as a Postal Inspector that some methamphetamine users participate in mail theft, and check and credit card fraud to fund their purchases of methamphetamine.

19. Further, based upon my training, investigative experience and the facts presented in this affidavit, I believe probable cause exists that the electronic devices identified in ATTACHMENT A and paragraphs 12 and 15 of this affidavit were used in furtherance of this scheme. I have learned from my training and investigative experience that:

a. Individuals engaged in mail theft, check counterfeiting and fraud, and credit card fraud and identity theft typically use computers and printers to create the counterfeit checks and IDs and print them out on blank check stock or blank IDs. Further, individuals engaged in credit card fraud and using PII to obtain credit cards and other lines of credit in the names of others must use a computer or electronic device that has access to the internet in order to complete the application in support of the fraudulent account.

b. Individuals engaged in mail theft, check counterfeiting, and credit card fraud commonly use hard drives or portable electronic storage devices in furtherance of their scheme to defraud. Such devices allow their users to store large amounts of data including pictures, video, and other information. Individuals involved in producing counterfeit checks and/or obtaining fraudulent credit accounts require a computer or other electronic storage device in order to retain images and data of the checks they are producing and printing or the accounts they have fraudulently applied for.

c. Individuals engaged in mail theft, check counterfeiting, and credit card fraud typically use phones to communicate with others involved in the scheme via telephone calls, text records, and/or social media account communication, and/or take photographs of checks, identification cards, stolen US Mail, other individuals and/or victims, or personal identifying information. Further, because many modern cellular

devices act similarly to a computer and can access the internet, these devices may contain internet search information related to credit card fraud and/or check fraud. Also, when using a cellular signal, cellular devices communicate with cell towers. Those towers are fixed to a particular location and the cellular device using that particular tower makes a record of that particular tower's use. Most individuals retain possession of their cellular device wherever they travel. This is also especially true with individuals involved in mail theft, check fraud, and credit card as having immediate access to a device that allows them to instantly communicate with others involved in the scheme is crucial to the success of the scheme. Accessing location data on a cellular phone associated to an individual involved in a mail theft, check fraud, and credit card fraud scheme can provide evidence of where mail theft, check fraud, and credit card fraud may have occurred. Further, because evidence exists that Pao Yang and others involved in the scheme are associated to methamphetamine use, the cellular devices may contain evidence of methamphetamine use and/or distribution in the form of photographs or suspected methamphetamine, paraphernalia, or US Currency, text message content related to the use and/or distribution of methamphetamine, and cellular location data that may identify the location of the source of controlled substances.

ELECTRONIC STORAGE AND FORENSIC ANALYSIS

20. Based on my knowledge, training, and experience, I know that the devices described in ATTACHMENT A can store information for long periods of time. Similarly, things that have been viewed via the Internet are typically stored for some period of time on the device. This information can sometimes be recovered with forensics tools.

21. As further described in ATTACHMENT B, this application seeks permission to locate electronically stored information that might serve as direct evidence of the crimes described on the warrant. Such evidence will consist of calling logs, contact list information, text message information, images and photographs, IP logs,

documents, spreadsheets, and internet query information that relate to the use of the property to communicate with others, including co-conspirators, or to gather (stolen US Mail), reproduce, or distribute counterfeit checks, negotiable monetary instruments, identification cards, credit cards, debit cards and PII. This evidence will also establish how the property was used, the purpose of its use, who used it, and when. There is probable cause to believe that this forensic electronic evidence might be on the device because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Forensic evidence on a device can also indicate who has used or controlled the device. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence.

b. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when.

c. The process of identifying the exact electronically stored information on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

d. Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium.

22. Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of the device consistent with the warrant. The examination may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might

expose many parts of the device to human inspection in order to determine whether it is evidence described by the warrant.

23. Because this warrant seeks only permission to examine devices already in law enforcement's possession, the execution of this warrant does not involve the physical intrusion on to a premises. Consequently, I submit there is reasonable cause for the Court to authorize execution of the warrant at any time in the day or night.

CONCLUSION

24. Based on the facts set forth in this affidavit, I believe probable cause exists to show that the devices described in ATTACHMENT A contain the items listed in ATTACHMENT B of this affidavit. Therefore I am seeking the issuance of a warrant to search the devices for the items described in ATTACHMENT B, in violation of 18 USC 1708, Mail Theft, 18 USC 514(a) Fictitious Obligations, 18 USC 1028A, Aggravated ID Theft, 18 USC 1029, Access Device Fraud, and 18 USC 371, Conspiracy.

1:19PM

Matthew B. Schmitz
U.S. Postal Inspector

Subscribed and sworn to before me telephonically on this 5 day of April, 2021.

The Honorable James R. Sickel
United States Magistrate Judge
Eastern District of Wisconsin

ATTACHMENT A: PROPERTY TO BE SEARCHED

1. A black MSI laptop computer.
2. A white Hp printer with serial number CN06A6P2X0.
3. A gray Motorolla Tracfone.
4. An LG Tracfone.
5. A T-Mobile Revvl cell phone.
6. A blue cell phone with a pop socket (a pop socket is essentially a knob on the back of the cell phone).
7. A black Apple iPhone.
8. A Samsung cell phone with IMEI 355181113973829.
9. A Samsung Tab S6 Lite computer tablet.
10. A Samsung Tab S7 computer tablet.
11. An Hp laptop with model number 15-dy207lwm.
12. A Notebook PC model GA5021.

These Devices are currently all located in the Eastern District of Wisconsin and in the possession of the Grand Chute Police Department in Grand Chute, WI. This warrant would authorize the forensic examination of the Devices for the purpose of identifying electronically stored data particularly described in Attachment B.

ATTACHMENT B: PARTICULAR THINGS TO BE SEIZED

1. All records on the Devices described in Attachment A that relate to violations of 18 USC 1708, Mail Theft, 18 USC 514(a) Fictitious Obligations, 18 USC 1028, Aggravated ID Theft, 18 USC 1029, Access Device Fraud, and 18 USC 371, Conspiracy, since August 1, 2020, including:

   a. Evidence of user attribution showing who used or owned the Device at the time the things described in this warrant were created, edited, or deleted, such as logs, phonebooks, saved usernames and passwords, documents, and browsing history;

   b. Call log history.

   c. Address book or contacts lists.

   d. Records of internet search activity including records involving the search or query of files related to the location of banks, "washing" counterfeit checks, producing counterfeit checks, applying for credit cards, loans, or lines of credit, producing identification cards, and mail theft.

   e. Records identifying any text messages or text message history.

   f. Records identifying the historical location of the Devices.

   g. Photographs or images depicting what is believed to be US Mail, checks, credit cards, banks, applications for credit cards, loans, or lines of credit, identification card information (an individual's face and/or PII), personal identifying information (PII), controlled substances and paraphernalia related to the use of controlled substances, and US Currency.

   h. Ledgers, logs, or spreadsheets.

   i. Records discussing mail theft, check fraud, credit card fraud, and controlled substance use.

2. As used above, the terms "records" and "information" include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as flash memory or other media that can store data) and any photographic form.